STATE OF ALABAMA

Information Technology Standard

Standard 670-01S1: Risk Assessment

1. INTRODUCTION:

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its life cycle. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

2. OBJECTIVE:

Establish the requirements for performing routine risk assessments of the State of Alabama computing environment to address external and internal threat agents.

3. SCOPE:

These requirements apply to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information system resources.

4. REQUIREMENTS:

Based on the recommendations of the National Institute of Standards and Technology (NIST) Special Publication 800-30: Risk Management Guide for Information Systems, State of Alabama risk assessment processes shall follow these nine steps:

4.1 SYSTEM CHARACTERIZATION

All State of Alabama information systems and the networks that provide system-to-system communication establishes the risk assessment boundaries for this risk management policy. The risk assessment process shall encompass the entire system processing environment including, but not limited to, the information system mission, hardware, software, system interfaces, personnel access, system and data criticality, and the level of protection required to maintain system and data integrity, confidentiality, and availability.

4.2 THREAT IDENTIFICATION

The risk assessment shall evaluate the security posture of State of Alabama information systems and networks against common threat elements to include: computer, human, environmental and nature.

4.3 VULNERABILITY IDENTIFICATION

The risk assessment, utilizing security checklists and vulnerability assessment toolsets, shall be used to identify vulnerabilities within the State of Alabama information systems and networks and associate the vulnerability with an identified threat category. The security checklist shall, at a minimum, cover the Management, Operational and Technical security control areas.

4.4 CONTROL ANALYSIS

The risk assessment shall evaluate the effectiveness of current technical and non-technical security controls. The control analysis will review the preventative and detective characteristics of the security controls.

4.5 LIKELIHOOD DETERMINATION

Based on the threat element motivation, vulnerability type and existing control measures, a Likelihood Rating will be assigned to the vulnerability as Low, Medium or High. The following Likelihood Level definitions will be applied:

Table 4-1: Likelihood Level Definitions

High	The threat source is highly motivated and sufficiently capable and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

4.6 IMPACT ANALYSIS

The risk assessment will provide, based on the loss of confidentiality, integrity and availability, what impact is possible to the State of Alabama information system. The Impact will be ranked in a Low, Medium and High level.

Table 4-2: Impact Level Definitions

High	Exercise of the vulnerability may: (1) result in the highly costly loss of major tangible assets or resources; (2) significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) result in human death or serious injury.
Medium	Exercise of the vulnerability may: (1) result in the costly loss of tangible assets or resources; (2) violate, harm, or impede an organization's mission, reputation, or interest; or (3) result in human injury.
Low	Exercise of the vulnerability may (1) result in the loss of some tangible assets or resources, or (2) noticeably affect an organization's mission, reputation, or interest.

4.7 RISK DETERMINATION

The risk assessment will utilize these three attributes in making a final risk determination to the information system or network:

- The likelihood of a given threat-source's attempting to exercise a given vulnerability
- The magnitude of the impact should a threat-source successfully exercise the vulnerability
- The adequacy of planned or existing security controls for reducing or eliminating risk.

The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact. The risk level matrix, table 4-3 below, shows how the overall risk ratings might be determined based on inputs from the threat likelihood and threat impact categories.

Table 4-3: Risk Level Matrix

Threat Likelihood	Impact		
	Low (1)	**Medium (5)**	**High (10)**
High (10)	Low 10	Medium 50	High 100
Medium (5)	Low 5	Medium 25	Medium 50
Low (1)	Low 1	Low 5	Low 10

High Risk: If an observation or finding is evaluated as a high risk (>50 to 100), there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.

Medium Risk: If an observation is rated as medium risk (>10 to 50), corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.

Low Risk: If an observation is described as low risk (1 to 10), the system's owner must determine whether corrective actions are still required or decide to accept the risk.

Depending on the organization's requirements and the granularity of risk assessment desired, some assessments may include additional likelihood or impact levels such as Very Low or Very High to generate a Very Low/Very High risk level. A "Very High" risk level may require possible system shutdown or stopping of all IT system integration and testing efforts.

4.8 CONTROL RECOMMENDATIONS

In order to reduce risk to an acceptable level, the risk assessment will provide risk remediation recommendations based on these factors:

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability

4.9 RESULTS DOCUMENTATION

A detailed report shall be prepared for senior management following the conclusion of the risk assessment. The report will describe the threats and vulnerabilities, measure the risk, and provide recommendations for control implementation.

5. ADDITIONAL INFORMATION:

5.1 POLICY

Information Technology Policy 670-01: Risk Management
http://isd.alabama.gov/policy/Policy_670-01_Risk_Management.pdf

5.2 RELATED DOCUMENTS

Information Technology Dictionary
http://isd.alabama.gov/policy/IT_Dictionary.pdf

Information Technology Standard 670-01S2: Risk Mitigation
http://isd.alabama.gov/policy/Standard_670-01S2_Risk_Mitigation.pdf

Signed by Art Bess, Assistant Director

6. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	12/12/2006	